



0745/61002

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Applicants : Gunter MARINGER et al.
Serial No. : 09/462,616
Filed : April 3, 2000
For : METHOD AND DEVICE FOR THE MUTUAL AUTHENTICATION
OF COMPONENTS IN A NETWORK USING THE CHALLENGE-
RESPONSE METHOD
Group : 2135
Examiner : Paula W. Klimach

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

TRANSMITTAL LETTER FOR APPLICANTS' BRIEF

Enclosed is Applicants' Appeal Brief in the above-identified application.

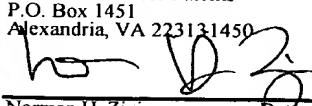
The fee of \$500.00 set by 37 C.F.R. § 41.20(b)(2) for filing the Brief is submitted herewith.

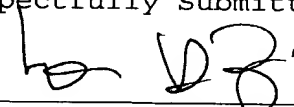
Please charge any additional fees incurred by reason of the Brief or credit any overpayment to Deposit Account No. 03-3125.

A duplicate of this Transmittal Letter is enclosed.

Respectfully Submitted,

Dated: September 18, 2006

I hereby certify that this paper is being deposited this date with the U.S. Postal Service as first class mail addressed to: Commissioner for Patents P.O. Box 1451 Alexandria, VA 22313-1450	
	9/18/06
Norman H. Zivin Reg. No. 25,385	


Norman H. Zivin
Registration No. 25,385
c/o Cooper & Dunham LLP
1185 Avenue of the Americas
New York, New York 10036
(212) 278-0400
Attorney for Applicants

500.00 07



0745/61002

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Applicants : Gunter MARINGER et al.
Serial No.: 09/462,616
Filed : April 3, 2000
For : METHOD AND DEVICE FOR THE MUTUAL AUTHENTICATION
OF COMPONENTS IN A NETWORK USING THE CHALLENGE-
RESPONSE METHOD
Group : 2135
Examiner : Paula W. Klimach

APPLICANTS' BRIEF

Applicants hereby submit this Brief in support of their appeal to the Board of Patent Appeals and Interferences from the Examiner's Final Rejection dated April 21, 2006, of claims 16-39 of this application.

TABLE OF CONTENTS

1.	Real Party in Interest	3
2.	Related Appeals and Interferences	4
3.	Status of Claims	5
4.	Status of Amendments	6
5.	Summary of Claimed Subject Matter	7
6.	Grounds of Rejection to be Reviewed on Appeal	9
7.	Arguments	10
	A. Claims 16-27 are patentable	10
	B. Claims 16-27 are patentable	10
	C. Claims 28-39 are patentable	13
	Conclusion	15
8.	Claims Appendix	16
9.	Evidence Appendix	22
10.	Related Proceedings Appendix	23

1. REAL PARTY IN INTEREST

This application will be assigned to T-Mobile Deutschland GmbH, Landgrabenweg 151, D-53227 Bonn, Germany.

2. RELATED APPEALS AND INTERFERENCES

There are no prior or pending appeals, judicial proceedings or interferences known to the Applicants which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in this pending appeal.

3. STATUS OF CLAIMS

This application was originally filed with 14 claims filed with the original specification on January 10, 2000. Claim 15 was added by an Amendment dated January 21, 2005. Claims 1-15 were canceled and claims 16-39 added by an Amendment dated July 19, 2005.

A final Office Action was mailed on April 21, 2006, rejecting claims 16-39. Claims 16-39 stand finally rejected and are the basis of this appeal.

4. STATUS OF AMENDMENTS

An Office Action was mailed on April 21, 2006 finally rejecting claims 16-39. No amendments were filed subsequent to the final rejection. Claims 16-39 stand finally rejected and are set forth in The Claims Appendix attached hereto.

5. SUMMARY OF CLAIMED SUBJECT MATTER

The invention as claimed in independent claim 16 relates to a method for mutual authentication of a terminal ("M" Figs. 1-3) and a network ("N" Figs. 1-3), comprising

receiving, at the network, a triplet data set from an authentication center ("AUC" Figs. 1-3), the triplet data set including a first random number (challenge 1), a first response (response 1) and a second response (response 2) (page 9, line 14-page 10, line 4);

sending the first random number (challenge 1) to the terminal (page 9, line 14-page 10, line 4);

receiving, from the terminal, a first calculated response, calculated by the terminal based on the first random number (challenge 1), wherein the first calculated response is used as a second challenge (challenge 2) (page 9, line 14-page 10, line 4);

authenticating the terminal by matching the first calculated response with the first response (response 1) (page 9, line 14-page 10, line 4);

sending the second response (response 2) to the terminal (page 9, line 14-page 10, line 4); and

wherein the network is authenticated by the terminal by matching a second calculated response, calculated by the terminal based on the first random number (challenge 1) with the second response (response 2) (page 9, line 14-page 10, line 4).

The invention as claimed in independent claim 28 relates to a method for mutual authentication of a terminal ("M" Figs. 1-3) and a network ("N" Figs. 1-3), comprising

receiving, at the network, a triplet data set from an authentication center, the triplet data set including a first random number (challenge 1), a first response (response 1) and a second response (response 2) (page 9, line 14-page 10, line 10);

sending the first random number (challenge 1) and the second response (response 2) to the terminal as a single data set (page 9, line 14-page 10, line 10);

receiving, from the terminal, a first calculated response, calculated by the terminal based on the first random number (challenge 1), wherein the first calculated response is used as a second challenge (challenge 2) (page 9, line 14-page 10, line 10);

authenticating the terminal by matching the first calculated response with the first response (response 1) (page 9, line 14-page 10, line 10); and

wherein the network is authenticated by the terminal by matching a second calculated response, calculated by the terminal based on the first random number (challenge 1) with the second response (response 2) (page 9, line 14-page 10, line 10).

6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 16-18, 20, 25-30, and 37-39 are patentable under 35 U.S.C. § 103(a) over A Logic of Authentication, SRC Research Report 39, February 28, 1989 ("Burrows") in view of An Efficient Authentication Protocol for Mobile Networks, Journal of Information Science and Engineering, pages 505-520, 1999 ("Shieh").

Whether claims 19 and 31 are patentable under 35 U.S.C. § 103(a) over Burrows in view of U.S. Patent No. 6,021,203 ("Douceur").

Whether claims 21-24, 32-35, and 36 are patentable under 35 U.S.C. § 103(a) over Burrows in view of U.S. Patent No. 5,544,245 ("Tsubakiyama").

7. ARGUMENT

A. INTRODUCTION

Embodiments of the present invention relate to the mutual authentication of a mobile terminal and a mobile network. The present invention employs a novel series of challenges and responses that result in mutual authentication that is faster and more secure than mutual authentication methods found in the art.

B. CLAIMS 16-27 ARE PATENTABLE UNDER 35 U.S.C. § 103(A) OVER BURROWS, IN VIEW OF SHIEH, DOUCEUR, OR TSUBAKIYAMA

Independent claim 16 relates to a method for mutual authentication of a terminal and a network. A triplet data set is received at the network from an authentication center. The triplet data set includes a first random number (challenge 1), a first response (response 1) and a second response (response 2). The first random number (challenge 1) is sent to the terminal. A first calculated response, sent by the terminal, is received. The first calculated response is calculated by the terminal based on the first random number (challenge 1). The first calculated response is used as a second challenge (challenge 2). The terminal is authenticated by matching the first calculated response with the first response (response 1). The second response (response 2) is sent to the terminal. The network is authenticated by the terminal by matching a second calculated response, calculated

by the terminal based on the first random number (challenge 1) with the second response (response 2).

In claim 16, an authentication procedure is carried out between two entities M and N where an Authentication Center Auc delivers authentication data to N. The Auc delivers a first random number (challenge 1), a first response (response 1) and a second response (response 2) to N.

The portions of Burrows cited in the April 21, 2006 Office Action relate to an explanation of the Needham-Schroeder Protocol (with shared keys) for authenticating two entities A and B and a server S, where S delivers authentication data to A.

It can be implied from the Office Action that the Examiner maintains that the entity "A" of Burrows corresponds to the entity "N" of claim 16, the entity "B" of Burrows corresponds to the entity "M" of claim 16, and that the server "S" of Burrows corresponds with the Auc of claim 16.

The Examiner also implies that $\{K_{AB}, A\}_{K_{BS}}$ corresponds to Challenge 1, K_{AB} corresponds to Response 1, and N_A corresponds to Response 2.

Put simply, the Examiner has laid out the following comparison:

A corresponds to N
 B corresponds to M
 S corresponds to Auc

$\{K_{AB}, A\}K_{BS}$	corresponds to	Challenge 1
K_{AB}	corresponds to	Response 1
N_A	corresponds to	Response 2

Using the Examiner's analysis above, a detailed comparison between the technique of Burrows and the method of claim 16 reveals that the two are not the same and that the technique of Burrows fails to teach or suggest the method of claim 16.

The table below is provided to help illustrate the correspondences between claim 16 and Burrows so that proper attention may be drawn to their differences.

Message	Claim 16	Needham-Schroeder Protocol (Burrows)
1. $A \rightarrow S$	Triplet Request	A, B, N_A
2. $S \rightarrow A$	Challenge 1, Response 1, Response 2 Challenge 1, Response 1, Response 2	$\{N_A, B, K_{AB}, \{K_{AB}, A\}K_{BS}\}K_{AS}$ $\{K_{AB}, A\}K_{BS}$ K_{AB} N_A
3. $A \rightarrow B$	Challenge 1	$\{K_{AB}, A\}K_{BS}$
4. $B \rightarrow A$	Response 1 = Challenge 2	$\{N_B\} K_{AB} \neq K_{AB}$
5. $A \rightarrow B$	Response 2	$\{N_B - 1\} K_{AB} \neq N_A$

In the table above, the 5 messages of Burrows taken from page 18 are overlaid with the comparable steps taken from

claim 16. It can be seen that steps 4 and 5 of Burrows differ from the corresponding steps of claim 16 because in message 4, Burrows transmits $\{N_B\}_{K_{AB}}$ while claim 16 uses Response 1 which is assumed to correspond to K_{AB} . Additionally, in message 5, Burrows transmits $\{N_B - 1\}_{K_{AB}}$ while claim 16 uses Response 2 which is assumed to correspond to N_A .

Accordingly, Burrows fails to teach or suggest the method for mutual authentication of a terminal and a network as claimed in independent claim 16. Additionally, neither Shieh, Douceur, nor Tsubakiyama teach the method steps of independent claim 16 that are argued to be absent from Burrows in the arguments above and the Office Action does not contend that they do. Accordingly, independent claim 16 along with dependent claims 17-27 are patentably distinct from the cited art.

C. CLAIMS 28-39 ARE PATENTABLE UNDER 35 U.S.C. § 103(A) OVER BURROWS, IN VIEW OF SHIEH, DOUCEUR, OR TSUBAKIYAMA

A similar comparison reveals that Burrows does not teach or suggest the method of independent claim 28:

Message	Claim 28	Needham-Schroeder Protocol (Burrows)
1. $A \rightarrow S$	Triplet Request	A, B, N_A
2. $S \rightarrow A$	Challenge 1, Response 1, Response 2 Challenge 1, Response 1, Response 2	$\{N_A, B, K_{AB}, \{K_{AB}, A\}_{K_{BS}}\}_{K_{AS}}$ $\{K_{AB}, A\}_{K_{BS}}$ K_{AB} N_A
3. $A \rightarrow B$	Challenge 1	$\{K_{AB}, A\}_{K_{BS}}$

	Response 2	No Response	$\neq N_A$
4. B \rightarrow A	Response 1 = Challenge 2	$\{N_B\} K_{AB}$	$\neq K_{AB}$

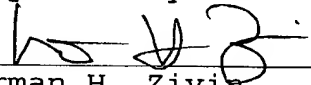
In the table above, the messages of Burrows taken from page 18 are overlaid with the comparable steps taken from claim 28. It can be seen that steps 3 and 4 of Burrows differ from the corresponding steps of claim 28 because in message 3, Burrows fails to transmit N_A which is assumed to correspond with Response 2. Additionally, in message 4, Burrows transmits $\{N_B\}K_{AB}$ while claim 28 uses Response 1=Challenge 2, which is assumed to correspond to K_{AB} .

Accordingly, Burrows fails to teach or suggest the method for mutual authentication of a terminal and a network as claimed in independent claim 28. Additionally, neither Shieh, Douceur, nor Tsubakiyama teach the steps of independent claim 28 that are argued to be absent from Burrows in the arguments above and the Office Action does not contend that they do. Accordingly, independent claim 28 along with dependent claims 29-39 are patentably distinct from the cited art.

The distinguishing features discussed above are significant. By utilizing the claimed novel series of challenges and responses, mutual authentication may be faster and more secure than mutual authentication methods found in the art.

CONCLUSION

A reversal of the Final Rejection of claims 16-39 by this Honorable Board is respectfully requested.

Respectfully submitted,
Dated: September 18, 2006 By 
Norman H. Zivin
Reg. No. 25,385
Cooper & Dunham LLP
1185 Avenue of the Americas
New York, NY 10036
Tel (212) 278-0400
Fax (212) 391-0630
Attorney for Applicants

NHZ/JBG

8. CLAIMS APPENDIX

Claim 1-15 (Canceled)

Claim 16. A method for mutual authentication of a terminal and a network comprising the steps of:

receiving, at the network, a triplet data set from an authentication center, the triplet data set including a first random number (challenge 1), a first response (response 1) and a second response (response 2);

sending the first random number (challenge 1) to the terminal;

receiving, from the terminal, a first calculated response, calculated by the terminal based on the first random number (challenge 1), wherein the first calculated response is used as a second challenge (challenge 2);

authenticating the terminal by matching the first calculated response with the first response (response 1);

sending the second response (response 2) to the terminal;
and

wherein the network is authenticated by the terminal by matching a second calculated response, calculated by the terminal based on the first random number (challenge 1) with the second response (response 2).

Claim 17. The method of claim 16, wherein the terminal

calculates the first calculated response from the first random number (challenge 1) using an internally stored key.

Claim 18. The method of claim 16, wherein the terminal calculates the second calculated response from the first random number (challenge 1) or from the first calculated response using an internally stored key.

Claim 19. The method of claim 16, wherein multiple triplet data sets are received from the authentication center and stored on the network as a stockpile to reduce the number of times triplet data sets must be received.

Claim 20. The method as claimed in claim 16, wherein to use the first calculated response of the terminal as the second challenge (Challenge 2), a shorter length of the first calculated response is filled out to make up a greater length of the second challenge (Challenge 2).

Claim 21. The method as claimed in claim 20, wherein the filling-out is performed on a subscriber-specific basis; and the complete length of the first calculated response is shortened before transmission.

Claim 22. The method as claimed in claim 20, wherein the

first calculated response is filled out with defined bits from an internally stored key to make up the length of the second challenge (Challenge 2).

Claim 23. The method as claimed in claim 20, wherein the second challenge (Challenge 2) corresponds to the first calculated response before it was shortened.

Claim 24. The method as claimed in claim 16, wherein the network is a GSM network.

Claim 25. The method as claimed in claim 16, wherein the network is a wire-based network.

Claim 26. The method as claimed in claim 25, wherein components in the wire-based network are different monitoring units of computers which authenticate themselves with a central computer, and vice versa.

Claim 27. The method as claimed in claim 16, wherein the authentication center calculates the triplet data sets requested by the network and transmits the calculated triplet data sets to the network off-line and independently of time, on request by the network, and before data interchange between the network and the terminal.

Claim 28. A method for mutual authentication of a terminal and a network comprising the steps of:

receiving, at the network, a triplet data set from an authentication center, the triplet data set including a first random number (challenge 1), a first response (response 1) and a second response (response 2);

sending the first random number (challenge 1) and the second response (response 2) to the terminal as a single data set;

receiving, from the terminal, a first calculated response, calculated by the terminal based on the first random number (challenge 1), wherein the first calculated response is used as a second challenge (challenge 2);

authenticating the terminal by matching the first calculated response with the first response (response 1); and

wherein the network is authenticated by the terminal by matching a second calculated response, calculated by the terminal based on the first random number (challenge 1) with the second response (response 2).

Claim 29. The method of claim 28, wherein the terminal calculates the first calculated response from the first random number (challenge 1) using an internally stored key.

Claim 30. The method of claim 28, wherein the terminal calculates the second calculated response from the first random number (challenge 1) or from the first calculated response using an internally stored key.

Claim 31. The method of claim 28, wherein multiple triplet data sets are received from the authentication center and stored on the network as a stockpile to reduce the number of times triplet data sets must be received.

Claim 32. The method as claimed in claim 28, wherein to use the first calculated response of the terminal as the second challenge (Challenge 2), a shorter length of the first calculated response is filled out to make up a greater length of the second challenge (Challenge 2).

Claim 33. The method as claimed in claim 32, wherein the filling-out is performed on a subscriber-specific basis; and the complete length of the first calculated response is shortened before transmission.

Claim 34. The method as claimed in claim 32, wherein the first calculated response is filled out with defined bits from an internally stored key to make up the length of the second challenge (Challenge 2).

Claim 35. The method as claimed in claim 32, wherein the second challenge (Challenge 2) corresponds to the first calculated response before it was shortened.

Claim 36. The method as claimed in claim 28, wherein the network is a GSM network.

Claim 37. The method as claimed in claim 28, wherein the network is a wire-based network.

Claim 38. The method as claimed in claim 37, wherein components in the wire-based network are different monitoring units of computers which authenticate themselves with a central computer, and vice versa.

Claim 39. The method as claimed in claim 28, wherein the authentication center calculates the triplet data sets requested by the network and transmits the calculated triplet data sets to the network off-line and independently of time, on request by the network, and before data interchange between the network and the terminal.

9. EVIDENCE APPENDIX

There was no evidence submitted pursuant to 37 C.F.R
1.130, 1.131, or 1.132.

10. RELATED PROCEEDINGS AND APPENDIX

None .